

H

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

C.A:04-1199 (SLR)

SRI INTERNATIONAL, INC.,)
a California Corporation)

Plaintiff and)
Counterclaim Defendant,)

v.)

INTERNET SECURITY SYSTEMS, INC.,)
a Delaware Corporation, INTERNET)
SECURITY SYSTEMS, INC., a Georgia)
Corporation, and SYMANTEC)
CORPORATION, a Delaware)
Corporation,)

Defendants and)
Counterclaim-Plaintiffs.)

-----)

COPY

VIDEOTAPED DEPOSITION

OF

Y. FRANK JOU

At Raleigh, North Carolina
January 27, 2006 - 9:53 a.m.

Reported by:
Debra D. Bowden

capitalreporting

PO Box 97696
Raleigh, NC 27624

8360 Six Forks Road
Suite 101
Raleigh, NC 27615

919.398.7775 ph
919.398.7741 fax

www.capreporting.com

capreporting@aol.com

170

1 meant -- what I meant was the capability we
2 implement was local in nature.

3 Q. Um-hmm.

4 A. And as the goal we try to achieve was to be
5 able to scale this capability to a global
6 label. So that was my intent in this
7 description here. Basically as a next step
8 in the capability it should be extend from
9 local to a global area. Global scope.
10 Yeah.

11 Q. Okay. And now the DARPA project was a
12 three-year project; correct?

13 A. Right.

14 Q. It was a limited in time; correct?

15 A. Yeah, um-hmm.

16 Q. And limited in funding money; correct?

17 A. Yeah.

18 Q. Had you had more time and money, would you
19 have taken that natural extension step to a
20 more global system?

21 A. Definitely that was in our intent. But you
22 know, again I should say this was a
23 research project. There was no guarantee,
24 you know, we would be able to bear any

1 fruit even though if the time or resource
2 is allowed at that point in time.
3 Q. If you go back to the architecture
4 document, J18, on page 3.
5 A. Page 3. Okay.
6 Q. And if you go to Section 2.1.
7 A. Um-hmm.
8 Q. And you go to the third paragraph.
9 A. Um-hmm.
10 Q. The middle of it. And you say, "While it
11 is not within the scope of this project, we
12 expect that the detection analysis
13 functions implemented in the local
14 subsystem can be extended to a global level
15 and correlate intrusion events among
16 several routers." Do you see that?
17 A. Um-hmm.
18 Q. And then it goes on to say, "The management
19 capability which is based on SNMP framework
20 can logically be further extended among
21 management nodes in a hierarchical fashion
22 to establish a status map for an autonomous
23 system."
24 A. Um-hmm.

1 Q. Now, while your DARPA project was limited
2 in time and funding, did you create the
3 design such that it could be extended in
4 this hierarchical fashion?

5 A. I would not say created, because the SNMP
6 network by its nature is to monitor remote
7 system.

8 Q. Um-hmm.

9 A. And be able to reflect a healthy -- the
10 healthy -- the status of the network, you
11 know, it's healthy, whether it's healthy or
12 it's, you know, under stress. That was the
13 intent of the SNMP framework. And our
14 thinking at that point in time was to take
15 advantage of this SNMP by the fact that
16 it's able to monitor several systems in a
17 distributive fashion. And you know, the
18 challenge at that point was how do you
19 correlate. I think that was the main
20 technical challenge at that point in time
21 in terms of how do you collect -- collect
22 of the local detection result was not an
23 issue. The issue was how do you come up
24 with the intelligence, how do you correlate

1 all the relevant information and be able
2 to, you know, derive a certain logical or
3 reasonable conclusion, and able to, based
4 upon this result, take action accordingly.
5 I think that was the challenge, and the --
6 you know, we did look into that aspect.
7 But however at that point we did not have a
8 very promising, you know, development at
9 that time. At the conclusion of the
10 project. So that was, you know, the open
11 question at that point.

12 Q. And if you just saw the term correlate --

13 A. Um-hmm.

14 Q. -- what would that mean to you?

15 MS. PRESCOTT: Objection to form.

16 A. Correlate means how do you put two or more
17 than two input together and derive
18 meaningful information, or intelligence,
19 out of these different infrastreams of
20 information, and be able to come up with
21 certain rationale or logic that what this,
22 you know, behavior manifests to itself.

23 Probably that's kind of lengthy or
24 wordy, but that's my understanding of this

I

REDACTED

J

REDACTED